IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

TQP DEVELOPMENT, LLC,
Plaintiff,
v.

1. **ALLIANZ LIFE INSURANCE COMPANY OF NORTH AMERICA;**
2. **AMERICAN FUNDS DISTRIBUTORS, INC.;**
3. **CHARLES SCHWAB & CO., INC.;**
4. **CNA FINANCIAL CORPORATION;**
5. **DODGE & COX;**
6. **FARMERS GROUP, INC;**
7. **FARMERS INSURANCE GROUP;**
8. **FEDERATED INVESTORS, INC.;**
9. **GEICO CORPORATION;**
10. **GOVERNMENT EMPLOYEES INSURANCE;**
11. **HSBC HOLDINGS PLC;**
12. **HSBC USA INC.;**
13. **JEFFERIES & COMPANY, INC.;**
14. **MURIEL SIEBERT & CO., INC.;**
15. **NATIONWIDE INVESTMENT SERVICES CORPORATION;**
16. **NATIONWIDE MUTUAL INSURANCE COMPANY;**
17. **OPPENHEIMERFUNDS, INC.;**
18. **PIPER JAFFRAY & CO.;**
19. **SCOTTRADE, INC.;**
20. **STATE FARM MUTUAL AUTOMOBILE INSURANCE COMPANY;**
21. **STATE STREET CORPORATION;**
22. **SUNTRUST BANKS, INC.;**
23. **THE CAPITAL GROUP COMPANIES, INC.; AND**
24. **THE TRAVELERS INDEMNITY COMPANY**

Defendants,

Civil Action No.

JURY TRIAL DEMANDED

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

This is an action for patent infringement in which TQP Development, LLC ("TQP") makes the following allegations against Allianz Life Insurance Company of North America; American Funds Distributors, Inc.; Charles Schwab & Co., Inc.; CNA Financial Corporation; Dodge & Cox; Farmers Group, Inc.; Farmers Insurance Group; Federated Investors, Inc.; Geico Corporation; Government Employees Insurance; HSBC Holdings plc; HSBC USA Inc.; Jefferies & Company, Inc.; Muriel Siebert & Co., Inc.; Nationwide Investment Services Corporation; Nationwide Mutual Insurance Company; OppenheimerFunds, Inc.; Piper Jaffray & Co.; Scottrade, Inc.; State Farm Mutual Automobile Insurance Company; State Street Corporation; SunTrust Banks, Inc.; The Capital Group Companies, Inc.; and The Travelers Indemnity Company (collectively, "Defendants"):

PARTIES

1. Plaintiff TQP Development, LLC is a Texas limited liability company having a principal place of business of 207C North Washington Street, Marshall, Texas 75670.

2. On information and belief, Defendant Allianz Life Insurance Company of North America ("Allianz") is a Minnesota corporation with its principal place of business at 5701 Golden Hills Dr., Minneapolis, MN 55416.

3. On information and belief, Defendant American Funds Distributors, Inc. ("American Funds") is a California corporation with its principal place of business at 333 S. Hope St., Floor 55, Los Angeles, CA 90071. American Funds has appointed Angela M. Mitchell, 333 S. Hope St., Floor 55, Los Angeles, CA 90071 as its agent for service of process.

4. On information and belief, Defendant Charles Schwab & Co., Inc. ("Schwab") is a California corporation with its principal place of business at 211 Main Street, San Francisco, CA 94105. Schwab has appointed CT Corporation System 818 W. Seventh St., Los Angeles, CA 90017 as its agent for service of process.

5. On information and belief, Defendant CNA Financial Corporation ("CNA") is a Delaware corporation with its principal place of business at 333 S. Wabash Ave., Chicago, IL 60604. CNA has appointed The Corporation Trust Company 1209 Orange St., Wilmington, DE 19801 as its agent for service of process.

6. On information and belief, Defendant Dodge & Cox is a California corporation with its principal place of business at 555 California St. Fl. 40, San Francisco, CA 94104. Dodge & Cox has appointed Thomas M. Mistele 555 California St. Fl. 40, San Francisco, CA 94104 as its agent for service of process.

7. On information and belief, Defendant Farmers Group, Inc. ("Farmers") is a Nevada corporation with its principal place of business at 4680 Wilshire Blvd, Los Angeles, CA 90010. Farmers has appointed CSC Services of Nevada 2215-B Renaissance Dr., Las Vegas, NV 89119 as its agent for service of process.

8. On information and belief, Farmers Insurance Group. ("FIG") is a Nevada corporation with its principal place of business at 4680 Wilshire Blvd, Los Angeles, CA 90010. FIG has appointed CSC Services of Nevada 2215-B Renaissance Dr., Las Vegas, NV 89119 as its agent for service of process.

9. On information and belief, Defendant Federated Investors, Inc. ("Federated") is a Pennsylvania corporation with its principal place of business at Federated Investors Tower, 1001 Liberty Ave., Pittsburgh, PA 15222.

10. On information and belief, Defendant Geico Corporation ("Geico") is a Delaware corporation with its principal place of business at One GEICO Plaza, Washington, D.C. 20076. Geico has appointed The Corporation Trust Company 1209 Orange St., Wilmington, DE 19801.

11. On information and belief, Defendant Government Employees Insurance ("GEI") is a Maryland corporation with its principal place of business at 5260 Western Ave., Chevy Chase, MD 20815. GEI has appointed The Corporation Trust Company 300 E. Lombard St., Baltimore, MD 21202 as its agent for service of process.

12. On information and belief, Defendant HSBC Holdings plc ("HSBC") is a British corporation with its principal place of business at 8 Canada Square, London, England E14 5HQ.

13. On information and belief, Defendant HSBC USA Inc. ("HSBC USA") is a Maryland corporation with its principal place of business at 452 Fifth Ave., New York 10018. HSBC USA has appointed The Corporation Trust, Inc. 351 W. Camden St., Baltimore, MD 21201 as its agent for service of process.

14. On information and belief, Defendant Jefferies & Company, Inc.("Jefferies") is a Delaware corporation with its principal place of business at 520 Madison Ave., 11th Floor, New York, NY 10022. Jefferies has appointed The Corporation Trust Company 1209 Orange St., Wilmington, DE 19801 as its agent for service of process.

15. On information and belief, Defendant Muriel Siebert & Co., Inc. ("Muriel Siebert") is a Delaware corporation with its principal place of business at 885 Third Ave.,

Suite 1720, New York, NY 10022. Muriel Siebert has appointed The Corporation Trust Company 1209 Orange St., Wilmington, DE 19801 as its agent for service of process.

16. On information and belief, Defendant Nationwide Investment Services Corporation ("NISC") is an Ohio corporation with its principal place of business at 1 West Nationwide Blvd., Columbus, OH 43215. NISC has appointed CT Corporation System 1300 East Ninth St., Cleveland, OH 44114 as its agent for service of process.

17. On information and belief, Defendant Nationwide Mutual Insurance Company ("Nationwide") is an Ohio corporation with its principal place of business at 1 West Nationwide Blvd., Columbus, OH 43215.

18. On information and belief, Defendant OppenheimerFunds, Inc. ("Oppenheimer") is a New York corporation with its principal place of business at 2 World Financial Center, 225 Liberty St., 11th Floor, New York, NY 10281. Muriel Siebert has appointed C T Corporation System 111 Eighth Ave., New York, New York, 10011 as its agent for service of process.

19. On information and belief, Defendant Piper Jaffray & Co. ("Piper Jaffray") is a Delaware corporation with its principal place of business at 800 Nicollet Mall, Minneapolis, MN 55402. Piper Jaffray has appointed The Corporation Trust Company 1209 Orange St., Wilmington, DE 19801 as its agent for service of process.

20. On information and belief, Defendant Scottrade, Inc. ("Scottrade") is an Arizona corporation with its principal place of business at 12800 Corporate Hill Dr., St. Louis, MO 63131. Scottrade has appointed CT Corporation System 2394 E. Camelback Rd., Phoenix, AZ 85016 as its agent for service of process.

21. On information and belief, Defendant State Farm Mutual Automobile Insurance Company ("State Farm") is an Illinois corporation with its principal place of business at 1 State Farm Plaza, Bloomington, IL 61710.

22. On information and belief, Defendant State Street Corporation ("State Street") is a Massachusetts corporation with its principal place of business at One Lincoln St., Boston, MA 02111. State Street has appointed CT Corporation System 155 Federal St., Suite 700, Boston, MA 02110 as its agent for service of process.

23. On information and belief, Defendant SunTrust Banks, Inc. ("SunTrust") is a Georgia corporation with its principal place of business at 303 Peachtree St., N.E., Atlanta, GA 30308. SunTrust has appointed Raymond D. Fortin 303 Peachtree St., N.E., Atlanta, GA 30308 as its agent for service of process.

24. On information and belief, Defendant The Capital Group Companies, Inc. ("Capital Group") is a California corporation with its principal place of business at 333 S. Hope Street, Los Angeles, CA 90071-1406. Capital Group has appointed Angela M Mitchell 333 S. Hope Street, Los Angeles, CA 90071-1406 as its agent for service of process.

25. On information and belief, Defendant The Travelers Indemnity Company ("Travelers") is a Connecticut corporation with its principal place of business at One Tower Square, Hartford, CT 06183.

JURISDICATION AND VENUE

26. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

27. Venue is proper in this district under 28 U.S.C. §§ 1391(c) and 1400(b). On information and belief, each Defendant has transacted business in this district, and has committed and/or induced acts of patent infringement in this district.

28. On information and belief, Defendants are subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statue, due at least to their substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

COUNT I

INFRINGEMENT OF U.S. PATENT NO. 5,412,730

29. Plaintiff is the owner by assignment of United States Patent No. 5,412,730 ("the '730 Patent") entitled "Encrypted Data Transmission System Employing Means for Randomly Altering the Encryption Keys." The '730 Patent issued on May 2, 1995. A true and correct copy of the '730 Patent is attached as Exhibit A

30. Upon information and belief, Defendant Allianz has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Allianz websites (including, without limitation to, www.allianzlife.com and www3.financialtrans.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Allianz and/or Allianz's customers connect to Allianz's website, a communication link is established between host servers and the client

computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Allianz's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Allianz provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Allianz generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Allianz encrypts data for transmission from the host server to the client. In addition, Allianz directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Allianz generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric

algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Allianz decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Allianz is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Allianz is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Allianz is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

31. Upon information and belief, Defendant American Funds has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various American Funds websites (including, without limitation to, www.americanfunds.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when American Funds and/or American Funds' customers connect to American Funds' website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of American Funds' website, client

computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. American Funds provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. American Funds generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. American Funds encrypts data for transmission from the host server to the client. In addition, American Funds directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. American Funds generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. American Funds decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a

user of the client computer. By virtue of performing each step of the claimed method, Defendant American Funds is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant American Funds is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant American Funds is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

32. Upon information and belief, Defendant Schwab has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Schwab websites (including, without limitation to, client.schwab.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Schwab and/or Schwab's customers connect to Schwab's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Schwab's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Schwab provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and

decrypt data. Schwab generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Schwab encrypts data for transmission from the host server to the client. In addition, Schwab directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Schwab generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Schwab decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Schwab is directly infringing the ‘730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Schwab is directly infringing, literally infringing, and/or infringing the ‘730 Patent under the doctrine of

equivalents. Defendant Schwab is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

33. Upon information and belief, Defendant CNA has been and now is infringing the ‘730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various CNA websites (including, without limitation to, www.cna.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the ’730 Patent to the injury of TQP. For example, when CNA and/or CNA’s customers connect to CNA’s website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of CNA’s website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. CNA provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. CNA generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced

at a time dependent upon a predetermined characteristic of the data being transmitted over said link. CNA encrypts data for transmission from the host server to the client. In addition, CNA directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. CNA generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. CNA decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant CNA is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant CNA is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant CNA is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

34. Upon information and belief, Defendant Dodge & Cox has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Dodge & Cox websites (including, without limitation to, www.dodgeandcox.com) for transmitting data

comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Dodge & Cox and/or Dodge & Cox's customers connect to Dodge & Cox's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Dodge & Cox's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Dodge & Cox provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Dodge & Cox generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Dodge & Cox encrypts data for transmission from the host server to the client. In addition, Dodge & Cox directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Dodge & Cox generates, or directs the client computer to generate, a second

sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Dodge & Cox decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Dodge & Cox is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Dodge & Cox is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Dodge & Cox is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

35. Upon information and belief, Defendant Farmers has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Farmers websites (including, without limitation to, eagent.farmersinsurance.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Farmers and/or Farmers' customers connect to Farmers' website, a communication link is established between host servers and the client computer. Data transmitted over

this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Farmers' website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Farmers provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Farmers generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Farmers encrypts data for transmission from the host server to the client. In addition, Farmers directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Farmers generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key

values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Farmers decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Farmers is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Farmers is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Farmers is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

36. Upon information and belief, Defendant FIG has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various FIG websites (including, without limitation to, eagent.farmersinsurance.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when FIG and/or FIG's customers connect to FIG's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of FIG's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is

established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. FIG provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. FIG generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. FIG encrypts data for transmission from the host server to the client. In addition, FIG directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. FIG generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. FIG decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant FIG is directly infringing the ‘730 Patent. In addition,

by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant FIG is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant FIG is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

37. Upon information and belief, Defendant Federated has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Federated websites (including, without limitation to, www.federatedinvestors.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Federated and/or Federated's customers connect to Federated's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Federated's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Federated provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Federated generates, or directs the client computer to generate, a first sequence of pseudo-random

key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Federated encrypts data for transmission from the host server to the client. In addition, Federated directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Federated generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Federated decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Federated is directly infringing the ‘730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Federated is directly infringing, literally infringing, and/or infringing the ‘730 Patent under the doctrine of equivalents. Defendant Federated is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

38. Upon information and belief, Defendant Geico has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Geico websites (including, without limitation to, service.geico.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Geico and/or Geico's customers connect to Geico's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Geico's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Geico provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Geico generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Geico encrypts data for transmission from the host server to the client. In

addition, Geico directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Geico generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Geico decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Geico is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Geico is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Geico is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

39. Upon information and belief, Defendant GEI has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various GEI websites (including, without limitation to, service.geico.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when GEI and/or GEI's

customers connect to GEI's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of GEI's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. GEI provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. GEI generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. GEI encrypts data for transmission from the host server to the client. In addition, GEI directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. GEI generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that

said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. GEI decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant GEI is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant GEI is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant GEI is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

40. Upon information and belief, Defendant HSBC has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various HSBC websites (including, without limitation to, www.us.hsbc.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when HSBC and/or HSBC's customers connect to HSBC's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of HSBC's

website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. HSBC provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. HSBC generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. HSBC encrypts data for transmission from the host server to the client. In addition, HSBC directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. HSBC generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. HSBC decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By

virtue of performing each step of the claimed method, Defendant HSBC is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant HSBC is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant HSBC is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

41. Upon information and belief, Defendant HSBC USA has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various HSBC USA websites (including, without limitation to, www.us.hsbc.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when HSBC USA and/or HSBC USA's customers connect to HSBC USA's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of HSBC USA's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. HSBC USA provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses

the same key to encrypt and decrypt data. HSBC USA generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. HSBC USA encrypts data for transmission from the host server to the client. In addition, HSBC USA directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. HSBC USA generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. HSBC USA decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant HSBC USA is directly infringing the ‘730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant HSBC USA is directly infringing, literally infringing, and/or infringing the ‘730 Patent under the doctrine of equivalents.

Defendant HSBC USA is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

42. Upon information and belief, Defendant Jefferies has been and now is infringing the ‘730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Jefferies websites (including, without limitation to, lfres.jefferies.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the ’730 Patent to the injury of TQP. For example, when Jefferies and/or Jefferies’ customers connect to Jefferies’ website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Jefferies’ website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Jefferies provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Jefferies generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value

in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Jefferies encrypts data for transmission from the host server to the client. In addition, Jefferies directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Jefferies generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Jefferies decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Jefferies is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Jefferies is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Jefferies is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

43. Upon information and belief, Defendant Muriel Siebert has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Muriel Siebert

websites (including, without limitation to, www.siebertnet.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Muriel Siebert and/or Muriel Siebert's customers connect to Muriel Siebert's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Muriel Siebert's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Muriel Siebert provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Muriel Siebert generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Muriel Siebert encrypts data for transmission from the host server to the client. In addition, Muriel Siebert directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over

the link. Muriel Siebert generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Muriel Siebert decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Muriel Siebert is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Muriel Siebert is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Muriel Siebert is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

44. Upon information and belief, Defendant NISC has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various NISC websites (including, without limitation to, myplan.nwservicecenter.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when NISC and/or NISC's customers connect to NISC's website, a communication link is established

between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of NISC's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. NISC provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. NISC generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. NISC encrypts data for transmission from the host server to the client. In addition, NISC directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. NISC generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric

algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. NISC decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant NISC is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant NISC is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant NISC is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

45. Upon information and belief, Defendant Nationwide has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Nationwide websites (including, without limitation to, myplan.nwservicecenter.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Nationwide and/or Nationwide's customers connect to Nationwide's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Nationwide's website, client computers must

agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Nationwide provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Nationwide generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Nationwide encrypts data for transmission from the host server to the client. In addition, Nationwide directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Nationwide generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Nationwide decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By

virtue of performing each step of the claimed method, Defendant Nationwide is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Nationwide is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Nationwide is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

46. Upon information and belief, Defendant Oppenheimer has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Oppenheimer websites (including, without limitation to, www.oppenheimerfunds.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Oppenheimer and/or Oppenheimer's customers connect to Oppenheimer's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Oppenheimer's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Oppenheimer provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a

symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Oppenheimer generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Oppenheimer encrypts data for transmission from the host server to the client. In addition, Oppenheimer directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Oppenheimer generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Oppenheimer decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Oppenheimer is directly infringing the ‘730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Oppenheimer is directly infringing, literally infringing, and/or infringing

the ‘730 Patent under the doctrine of equivalents. Defendant Oppenheimer is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

47. Upon information and belief, Defendant Piper Jaffray has been and now is infringing the ‘730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Piper Jaffray websites (including, without limitation to, online.piperjaffray.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the ’730 Patent to the injury of TQP. For example, when Piper Jaffray and/or Piper Jaffray’s customers connect to Piper Jaffray’s website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Piper Jaffray’s website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Piper Jaffray provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Piper Jaffray generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client

computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Piper Jaffray encrypts data for transmission from the host server to the client. In addition, Piper Jaffray directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Piper Jaffray generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Piper Jaffray decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Piper Jaffray is directly infringing the ‘730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Piper Jaffray is directly infringing, literally infringing, and/or infringing the ‘730 Patent under the doctrine of equivalents. Defendant Piper Jaffray is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

48. Upon information and belief, Defendant Scottrade has been and now is infringing the ‘730 Patent in the State of Texas, in this judicial district, and elsewhere in

the United States, by, among other things, methods practiced on various Scottrade websites (including, without limitation to, trading.scottrade.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Scottrade and/or Scottrade's customers connect to Scottrade's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Scottrade's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Scottrade provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Scottrade generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Scottrade encrypts data for transmission from the host server to the client. In addition, Scottrade directs the client computer to encrypt data comprising information sent from the client to the host server before it is

transmitted over the link. Scottrade generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Scottrade decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Scottrade is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Scottrade is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Scottrade is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

49. Upon information and belief, Defendant State Farm has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various State Farm websites (including, without limitation to, online.statefarm.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when State Farm and/or State Farm's customers connect to State Farm's website, a communication

link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of State Farm's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. State Farm provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. State Farm generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. State Farm encrypts data for transmission from the host server to the client. In addition, State Farm directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. State Farm generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that

said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. State Farm decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant State Farm is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant State Farm is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant State Farm is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

50. Upon information and belief, Defendant State Street has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various State Street websites (including, without limitation to, my.statestreet.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when State Street and/or State Street's customers connect to State Street's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are

encrypted according to the claimed method. In order to communicate with encrypted portions of State Street's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. State Street provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. State Street generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. State Street encrypts data for transmission from the host server to the client. In addition, State Street directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. State Street generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. State Street decrypts data sent from the client in order to use the data, and directs the

client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant State Street is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant State Street is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant State Street is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

51. Upon information and belief, Defendant Suntrust has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Suntrust websites (including, without limitation to, www.suntrust.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Suntrust and/or Suntrust's customers connect to Suntrust's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Suntrust's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the

host server. Suntrust provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Suntrust generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Suntrust encrypts data for transmission from the host server to the client. In addition, Suntrust directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Suntrust generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Suntrust decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Suntrust is directly infringing the ‘730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant

Suntrust is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Suntrust is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

52. Upon information and belief, Defendant Capital Group has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Capital Group websites (including, without limitation to, www.americanfunds.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Capital Group and/or Capital Group's customers connect to Capital Group's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Capital Group's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Capital Group provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Capital Group generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data,

based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Capital Group encrypts data for transmission from the host server to the client. In addition, Capital Group directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Capital Group generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Capital Group decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Capital Group is directly infringing the ‘730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Capital Group is directly infringing, literally infringing, and/or infringing the ‘730 Patent under the doctrine of equivalents. Defendant Capital Group is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

53. Upon information and belief, Defendant Travelers has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Travelers websites (including, without limitation to, pijas.travelers.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Travelers and/or Travelers' customers connect to Travelers' website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Travelers' website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Travelers provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Travelers generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Travelers encrypts data for transmission

from the host server to the client. In addition, Travelers directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Travelers generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Travelers decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Travelers is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Travelers is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Travelers is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

54. On information and belief, to the extent any marking was required by 35 U.S.C. §287, all predecessors in interest to the '730 Patent complied with any such requirements.

55. To the extent that facts learned in discovery show that Defendants' infringement of the '730 Patent is, or has been willful, Plaintiff reserves the right to request such a finding at the time of trial.

56. As a result of these Defendants' infringement of the '730 Patent, Plaintiff has suffered monetary damages and is entitled to a money judgment in an amount adequate to compensate for Defendants' infringement, but in no event less than a reasonable royalty for the use made of the invention by Defendants, together with interest and costs as fixed by the court, and Plaintiff will continue to suffer damages in the future unless Defendants' infringing activities are enjoined by this Court.

57. Unless a permanent injunction is issued enjoining these Defendants and their agents, servants, employees, representatives, affiliates, and all others acting on in active concert therewith from infringing the '730 Patent, Plaintiff will be greatly and irreparably harmed.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter:

1. A judgment in favor of Plaintiff that Defendants have infringed, directly, jointly and/or indirectly, by way of inducing and/or contributing to the infringement of the '730 Patent, and that such infringement was willful;

2. A permanent injunction enjoining Defendants and their officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in active concert therewith from infringement, inducing the infringement of, or contributing to the infringement of the '730 Patent;

3. A judgment and order requiring Defendants to pay Plaintiff its damages, costs, expenses, and prejudgment and post-judgment interest for Defendants' infringement of the '730 Patent as provided under 35 U.S.C. § 284;

4. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees; and

5. Any and all other relief, at law or equity, to which Plaintiff may show itself to be entitled.

DEMAND FOR JURY TRIAL

Relator, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

Dated: May 6, 2011

Respectfully submitted,

By: \s\ *Andrew Spangler*
Andrew Wesley Spangler
Spangler Law PC
208 N. Green St., Suite 300
Longview, TX 75601
903-753-9300
Fax: 903-553-0403
Email: spangler@spanglerlawpc.com

Marc Fenster
mfenster@raklaw.com
Andrew D Weiss
Email: aweiss@raklaw.com
Adam Hoffman
Email: ahoffman@raklaw.com
Alexander Giza
Email: agiza@raklaw.com
Russ August & Kabat
12424 Wilshire Boulevard, 12th Floor
Los Angeles, CA 90025
310-826-7474
Fax: 310-826-6991

Hao Ni
Texas Bar No. 24047205
Ni Law Firm, PLLC
3102 Maple Ave. Suite 400
Dallas, TX 75201
Telephone: (214) 800-2208
Fax: (214) 880-2209
E-mail: hni@nilawfirm.com

Attorneys for Plaintiff
TQP Development, LLC